

Morgan Lewis

National Financial
Risk & Regulatory Client Webinar

June 25, 2008

Proposed Regulation S-P Amendments

Steven Stone
Mark Matthews
Shauna Sappington

- www.morganlewis.com

Current Focus

- Risks of data breaches continue to threaten companies, employees and consumers
- Brokers and advisers face varying state data breach notification requirements
- Recent SEC enforcement action involving *NEXT Financial* has focused attention on releases of customer information when representatives shift firms
- To clarify firms' obligations, the SEC recently proposed changes to Regulation S-P that, if adopted, will
 - Impose national information securities program and data breach notice requirements
 - Allow limited sharing of personal information with departing employee's new firms

Background on Regulation S-P

- Regulation S-P was adopted in June 2000 to set forth requirements for safeguarding and disposing of customer information
- The safeguard rule requires firms to:
 - Adopt written policies and procedures for administrative, technical and physical safeguards to protect customer records and information
 - Provide customers with notice of the firms' privacy policy and the opportunity to opt out from having their information shared with nonaffiliated third parties
- The disposal rule requires firms to properly dispose of consumer information
- Regulation S-P does not:
 - Provide guidance on preparing for or responding to data breaches
 - Address information sharing when representatives shift firms

Proposed Changes to Regulation S-P

- On March 4, 2008, the SEC proposed changes to Regulation S-P that, if adopted, would
 - Expand the scope of the safeguard and disposal rules
 - Establish specific requirements for establishing a comprehensive program for safeguarding information and responding to data breaches
 - Clarify that key obligations arise only where unauthorized access or use would result in ***substantial harm or inconvenience*** to customer
 - Add an exception from the notice and opt out requirements for the limited disclosure of personal information relating to an employee moving to another firm

Clean up of Defined Terms

- Personal Information
 - The safeguards and disposal rules were adopted at different times and cover different information
 - *The safeguarding rule currently applies to “customer records and information”*
 - *The disposal rule applies to “consumer report information”*
 - *The notice and opt out requirements limits firms from sharing “nonpublic information”*
 - The proposed changes would amend these rules so both would protect “personal information,” which would include “nonpublic information” and “consumer report information” as well as any information of any individual consumer, employee, investor or security holder that is handled or maintained by or on behalf of the firm
- Sensitive Personal Information
 - The proposed changes would define “sensitive personal information” as “any personal information, or any combination of components of personal information, that would allow an unauthorized person to use, log into, or access an individual’s account, or to establish a new account using the individual’s identifying information”
- Substantial Harm or Inconvenience
 - The proposed rule change would define this as “personal injury, or more than trivial financial loss, expenditure of effort or loss of time”

Proposed Comprehensive Information Security Program

- Each firm would be required to create a program for safeguarding and responding to unauthorized access to or use of *personal information*
 - The proposed changes would require that each firm's program be designed to protect ***personal information*** from any anticipated security threats and unauthorized access to or use resulting in ***substantial harm or inconvenience*** to any consumer, employee, investor or security holder who is a natural person

Proposed Comprehensive Information Security Program - Components

1. Designate in writing an employee or employees to coordinate the program
2. Adopt written policies and procedures
3. Identify in writing reasonably foreseeable security risks that could result in unauthorized disclosure, misuse, alteration, destruction or other compromise of *personal information* or *personal information systems*
4. Design, document and implement information safeguards to control identified risks
5. Regularly test or otherwise monitor and document in writing the effectiveness of the safeguards' key controls, systems and procedures, including:
 - Effectiveness of access controls on personal information systems
 - Controls to detect, prevent and respond to attacks, or intrusions by unauthorized persons
 - Employee training and supervision
6. Train staff to implement the information security program
7. Oversee service providers by taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for the personal information at issue, and require service providers by contract to implement and maintain appropriate safeguards
8. Evaluate and adjust information security programs to reflect the results of the testing and monitoring, relevant technology changes, material changes to operations or business arrangements, and any other circumstances that the firm knows or reasonably believes may have a material impact on the program

Procedures for Responding to Breaches

1. Assess incidents involving unauthorized access or use, and identify in writing what types of personal information may have been compromised
2. Take steps to contain and control the incident to prevent further unauthorized access or use and document such steps in writing
3. Promptly conduct a reasonable investigation and determine in writing the likelihood that the information has been or will be misused after the firm becomes aware of any unauthorized access to *sensitive personal information*
4. Notify individuals with whom the information is identified as soon as possible (and document such notice) if the institution determines that misuse of information has occurred or is reasonably possible
5. Notify the SEC (or DEA) as soon as possible on Form SP-30 if the affected individual has suffered ***substantial harm or inconvenience*** or if the information was intentionally accessed or used by an unauthorized individual

Proposed Notice Requirements

- Description of the incident and the type of information compromised, what was done to protect the information from further unauthorized access or use
- Toll-free telephone number or other contact information for further information and assistance from the institution
- Recommendation that the individual review account statements and immediately report any suspicious activity to the institution
- Information about FTC guidance and FTC's website and telephone number

Proposed Changes Affecting Personnel

- Covered Persons - Natural persons who are
 - Associated persons of a broker-dealer
 - Supervised persons of a registered investment adviser
 - Associated persons of a registered transfer agent
- Proposed changes would
 - Extend the disposal rule to these covered persons
 - Carve out from customer notice and opt out requirements disclosure of certain information when a covered person moves between firms
 - *This exception would allow firms with departing persons to share limited customer information with the person's new firm*
 - *Permitted Information*
 - Customer's name
 - General description of the account type and products held by the customer
 - Contact information, including address, telephone number & e-mail address
 - *Firms relying on this exception must obtain and maintain a written request from the departing person for the information that would be disclosed*

Steps for Handling Potential Data Breaches

1. Assess the Breached Information
2. Mitigate Further Risk to Customer Information
3. Assess the Need to Alert Law Enforcement Agencies and File a Suspicious Activity Report
4. Consider Contacting SEC or SROs
5. Assess Customer Notification Obligations
6. Carefully Draft Customer Notification
7. Develop a Distribution Plan
8. Inform and Educate Your Client Service Representatives
9. Develop Press/Media “Talking Points”
10. Assess Insurance Needs

Morgan, Lewis & Bockius LLP



Steven Stone
Partner
202.739.5453
sstone@morganlewis.com



Mark Matthews
Partner
202.739.5655
mmatthews@morganlewis.com



Shauna Sappington
Associate
202.739.5573
ssappington@morganlewis.com

Additional Information

- SEC Proposed Rule Changes to Regulation S-P:
<http://sec.gov/rules/proposed/2008/34-57427fr.pdf>
- Morgan Lewis Law Flash – “SEC Proposes Amendments to Regulation S-P”:
http://www.morganlewis.com/pubs/IMFYI_AmendmentsRegS-P_11mar08.pdf
- “Responding to Data Breaches in the Securities and Investment Management Industry” by Steve Stone and Shauna Sappington:
http://www.morganlewis.com/pubs/StoneSappington_DataBreaches-WSL-Nov06.pdf
- Federal Financial Institutions Examination Council “Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice”:
<http://www.fdic.gov/news/news/financial/2005/fil2705.pdf>

Morgan Lewis

Risk & Regulatory National Financial
Client Webinar

June 25, 2008

Proposed Regulation S-P Amendments

Steven Stone
Mark Matthews
Shauna Sappington

- www.morganlewis.com